MAG DATACENTERS, LLC ("FORTRUST")
SOC 2 Type 2 Report on FORTRUST's Enterprise Data Center and Colocation Services System and on the Design and Operating Effectiveness of its Controls Relevant to Security and Availability

October 1, 2014 through September 30, 2015

EKS&H
AUDIT | TAX | CONSULTING

FORTRUST

SOC 2 Type 2 Report on FORTRUST's Enterprise Data Center and Colocation Services System and on the Design and Operating Effectiveness of its Controls Relevant to Security and Availability

October 1, 2014 through September 30, 2015

TABLE OF CONTENTS

SECTION ONE

FORTRUST's Management Assertion 2

SECTION TWO

Independent Service Auditor's Report 5

SECTION THREE

Description of FORTRUST's Enterprise Data Center and Colocation Services System

Company Overview 9
Components of the System 10
Boundaries of the System 12
Processing Activities 13
Other Aspects of the Internal Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls that Are Relevant to the Services Provided and the Applicable Trust Services Criteria 20
Trust Services Criteria, Related Controls, and Tests of Controls 22
Changes to the System During the Period 22
Complementary User Entity Controls 23

SECTION FOUR

FORTRUST's Security and Availability Trust Principles and Related Controls and Independent Service Auditor's Description of Tests of Controls and Results of Tests

Introduction 26

Security and Availability Principles 27
- Organization and Management 27
- Communications 33
- Risk Management and Design and Implementation of Controls 41
- Monitoring of Controls 50
- Logical and Physical Access Controls 52
- System Operations 60
- Change Management 62
- Availability 66

SECTION FIVE

Other Information Provided by FORTRUST that is Not Covered by the Independent Service Auditor's Report

Introduction 70
FORTRUST's Disaster Recovery Plan 70

SECTION ONE

FORTRUST'S MANAGEMENT ASSERTION

FORTRUST'S MANAGEMENT ASSERTION REGARDING ITS ENTERPRISE DATA CENTER AND COLOCATION SERVICES SYSTEM

We have prepared the description in Section Three titled "Description of Mag Datacenters, LLC ("FORTRUST") Enterprise Data Center and Colocation Services System," Throughout the period from October 1, 2014 to September 30, 2015 (the "Description"), based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2 ®)* (the "Description Criteria"). The Description is intended to provide users with information about the Enterprise Data Center and Colocation Services System (the "System"), particularly System controls intended to meet the criteria for the security and availability principles set forth in TSP Section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*). We confirm, to the best of our knowledge and belief, that:

a. The Description fairly presents FORTRUST's System throughout the period October 1, 2014 to September 30, 2015 based on the following Description Criteria:

   i. The Description contains the following information:

      (1) The types of services provided.

      (2) The components of the System used to provide the services, which are the following:

         (a) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

         (b) *Software*. The applicable programs and IT system software that support applicable programs (operating systems, middleware, and utilities).

         (c) *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

         (d) *Procedures*. The automated and manual procedures.

         (e) *Data*. The transaction streams, files, databases, tables, and output used or processed by a system.

      (3) The boundaries or aspects of the System covered by the Description.

      (4) If information is provided to, or received from, subservice organizations, or other parties

         (a) how such information is provided or received and the role of the subservice organization or other parties

         (b) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

      (5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following

         a) Complementary user entity controls contemplated in the design of the service organization's system.

         b) When the inclusive method is used to present a subservice organization, controls at the subservice organization.

(6) If the service organizations present the subservice organization using the carve-out method

(a) The nature of these services provided by the subservice organization

(b) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

(7) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons.

(8) In the case of a Type 2 report, relevant details of changes to the service organization's System during the period covered by the Description.

ii. The Description does not omit or distort information relevant to the service organization's System while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the System that each individual user may consider important to his or her own particular needs.

b. The controls stated in the Description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. The controls stated in the Description operated effectively throughout the period from October 1, 2014 to September 30, 2015 to meet the applicable trust services criteria.

FORTRUST does not use subservice organizations or other parties to address its Enterprise Data Center and Colocation Services System. Accordingly, our Description does not address the criteria in items (a)(i)(4) and (a)(i)(6).

Mag Datacenters, LLC
By: Steve Knudson
Chief Executive Officer
November 13, 2015

SECTION TWO

INDEPENDENT SERVICE AUDITOR'S REPORT

EKS&H
AUDIT | TAX | CONSULTING

7979 E. Tufts Avenue, Suite 400
Denver, Colorado 80237-2521
P: 303-740-9400
F: 303-740-9009
www.EKSH.com

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of
Mag Datacenters, LLC ("FORTRUST")
Denver, Colorado

Scope

We have examined the description in Section Three titled "Description of Mag Datacenters, LLC ("FORTRUST") Enterprise Data Center and Colocation Services System," throughout the Period From October 1, 2014 to September 30, 2015 (the "Description"), based on criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* ("Description Criteria") and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability, and confidentiality principles set forth in TSP Section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria)* (applicable trust services criteria), throughout the period from October 1, 2014 to September 30, 2015.

The Description indicates that certain applicable trust services criteria specified in the Description can be met only if complementary user entity controls contemplated in the design of FORTRUST's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section One, FORTRUST has provided its assertion titled "FORTRUST's Management Assertion," about the fairness of the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. FORTRUST is responsible for preparing the Description and the assertion, including the completeness, accuracy, and method of presentation of the Description and assertion; providing the services covered by the Description identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria, and stating them in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the Description Criteria set forth in FORTRUST's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the AICPA and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the Description Criteria, and (2) the controls were suitably designed and operated effectively to meet the applicable trust services criteria throughout the period October 1, 2014 to September 30, 2015.

To the Management of
Mag Datacenters, LLC ("FORTRUST")

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves:

- Evaluating and performing procedures to obtain evidence about whether the Description is fairly presented based on the Description Criteria, and the controls were suitably designed and operating effectively, to meet the applicable trust services criteria throughout the period from October 1, 2014 to September 30, 2015.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the Description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the services organizations in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations
Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in providing services. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design or operating effectiveness of the controls is subject to risks that the System may change or that controls at a service organization may become ineffective or fail.

Opinion
In our opinion, in all material respects, based on the Description and the applicable trust services criteria:

a. The Description fairly presents the System that was designed and implemented throughout the period October 1, 2014 to September 30, 2015.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period October 1, 2014 to September 30, 2015, and user entities applied the complementary user entity controls contemplated in the design of Ping's controls throughout the period from October 1, 2014 to September 30, 2015.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period October 1, 2014 to September 30, 2015, if user entities applied the complementary user entity controls contemplated in the design of Ping's controls operated effectively throughout the period from October 1, 2014 to September 30, 2015.

Description of Tests of Controls
The specific controls tested and the nature, timing, and results of those tests are presented in Section Four of our report titled "FORTRUST's Security and Availability Trust Principles and Related Controls and Independent Service Auditor's Description of Tests of Controls and Results of Tests."

The information attached to the Description in Section Five, "Other Information Provided by FORTRUST that is Not Covered by the Independent Service Auditor's Report," describes FORTRUST's Disaster Recovery Plan. It is presented by the management of FORTRUST to provide additional information and is not a part of FORTRUST's Description of its System made available to user entities during the period from October 1, 2014 to September 30, 2015. Information about FORTRUST's Disaster Recovery Plan has not been subjected to the procedures applied in the examination of the Description of the System and the suitability of the design and operating effectiveness to meet the related criteria stated in the Description of the System.

To the Management of
Mag Datacenters, LLC ("FORTRUST")

Restricted Use

This report and the description of tests of controls and results thereof in Section Four are intended solely for the information and use of FORTRUST; user entities of FORTRUST's Enterprise Data Center and Colocation Services System during some or all of the period October 1, 2014 to September 30, 2015; and prospective user entities, independent auditors, and practitioners providing services to such user entities; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's System interacts with user entities or other parties
- Internal control and its limitations
- Complementary user entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties. If report recipients are other than these specified parties (herein referred to as "non-specified users") and have obtained this report or have access to it, use of this report is the non-specified users' sole responsibility and at the non-specified users' sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against EKS&H LLLP as a result of such access. Further, EKS&H LLLP does not assume any duties or obligations to any non-specified users who obtain this report and/or have access to it.

EKS&H LLLP

EKS&H LLLP

November 13, 2015
Denver, Colorado

SECTION THREE

DESCRIPTION OF FORTRUST'S ENTERPRISE DATA CENTER AND COLOCATION SERVICES SYSTEM

COMPANY OVERVIEW

FORTRUST (the "Company") provides enterprise data center and colocation services in Denver, Colorado. This report describes certain controls that comprise the internal control system of FORTRUST's colocation services for data center customers at the Denver, Colorado, location. For customers who have specifically contracted for colocation services at the Denver Data Center facility (the "Data Center"), these elements include physical access, environmental safeguards, network availability (including network devices, information security, and change management), and customer ticketing. Its purpose is to assist FORTRUST customers and their independent auditors in determining the adequacy of the internal control system within FORTRUST to the extent that such controls have a direct effect on customers' processes and their control activities.

Because this Description of the System is intended to focus exclusively on the internal control system of FORTRUST relevant to its colocation services customers, it does not encompass all aspects of the services provided or procedures followed by FORTRUST. The report excludes Managed Services performed by outside third parties for FORTRUST or its customers. In addition, this report excludes FORTRUST's Data Center 2.0 deployment utilizing IO.Anywhere® Data Modules in Phoenix and New Jersey. Further, this report is not intended to cover the control aspects of customer systems or of the control aspects of FORTRUST's internal back-office network.

This report was developed to cover the majority of FORTRUST's colocation services customers. Therefore, it focuses on the significant information system general controls that are common for colocation customers. Any unique customer situations are outside the scope of this report.

Business and Organization

FORTRUST was founded in October 2000 to provide high availability enterprise data center and colocation services to the business community. Privately owned, FORTRUST offers flexibility and financial stability. FORTRUST provides the network connectivity, data center services, and physical security to handle customers' data center requirements. FORTRUST's 224,000 square foot facilities and flagship Data Center was built for a wide range of customers, from those needing just a single cabinet to large enterprises looking for several thousand square feet in which to relocate their entire data center operations. The Data Center features premium 36" raised floors that contain a maintenance-tolerant cooling system supporting high density power needs.

FORTRUST provides a secure, dedicated managed environment in which customers colocate their Internet, data networking, and voice equipment. Customers gain the flexibility to administer and access their own equipment while taking advantage of FORTRUST's electrical and environmental infrastructure, network performance, physical security, and scalability.

FORTRUST provides customers with secure, high availability direct Internet connectivity to a customer cabinet or rack via one or more fiber network connections. The "FORTRUST Network" means the FORTRUST owned and operated Internet Protocol ("IP") routing infrastructure for its Managed Internet Access service, consisting solely of FORTRUST measurement devices at selected FORTRUST points in its infrastructure and the connections between them in the FORTRUST Data Center. FORTRUST uses multiple-gigabit Ethernet circuits across diverse and multiple carriers for dedicated Internet access. FORTRUST uses border gateway protocol routing within its network, which automatically selects the shortest Internet route for traffic and limits downtime. The FORTRUST IP network connectivity distribution utilizes a fiber-optic backbone throughout the Data Center's raised floor areas. The network design utilizes a fully meshed network of switches and routers, which includes a diverse path redundancy built into both the "A" and "B" paths available to each cabinet or rack. Should one backbone link or upstream provider experience an outage, FORTRUST will automatically reroute traffic to the next available best path. Cabling can be structured above cabinets and suites or below the raised floor using pre-engineered cable and fiber management systems (e.g., ladder racks and fiber troughs).

Data Center Services

FORTRUST does not control customer-specific hardware, operating systems, databases, applications, or any other content loaded on the customer hardware. FORTRUST configures the customer site in a locked server cage, cabinet, or private room, which consists of multiple server racks that are based on each individual customer's specifications. FORTRUST is responsible for setting up each individual customer's environment, including the customer cages, cabinets, or, in some cases, a private room, providing network connectivity and power for the environment and managing the environmental safeguard systems. Once the customer environment has been established by FORTRUST, the customer is then responsible for building/staging the remaining Customer Provided Equipment infrastructure.

FORTRUST does not access customers' systems at the operating system, database, or application levels. As part of the FORTRUST service, when a customer is not able to be onsite at the FORTRUST center, FORTRUST provides Remote Hands services. Remote Hands services are defined as basic technical support services and are offered on a 24x7x365 basis. Remote Hands services are available to provide support for supervised first-line maintenance situations, which include fixes such as restarts (reboots) or card swaps (where cards are visible and accessible). The customer is responsible for clear equipment labeling, identification, and specific instructions on what is required.

COMPONENTS OF THE SYSTEM

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases, and tables)

The following sections of this Description define each of these five components comprising the System.

Infrastructure

The FORTRUST Data Center provides optimal conditions with constant temperature and humidity monitoring and redundant power supply (AC or DC). Among the services in the Data Center are continuous network monitoring and support, network redundancy into the Data Center with shadow and diverse redundancy options; customer support with a 24x7x365 Network Operations Center ("NOC") and onsite staffing; advanced security features, including biometric fingerprint scanners; and standardized entrance and delivery procedures. Customers can select a connection to FORTRUST's IP network from Fast Ethernet to Gigabit Ethernet. The Data Center provides onsite 24x7x365 Security personnel ("Security") and physical security procedures to protect customers' colocated equipment. FORTRUST does not access customer systems nor does it manage transaction processing, applications, databases, or operating systems on behalf of its customers.

In addition to the features listed above, FORTRUST's facility also includes a plug-and-play infrastructure that allows the ability to expand to meet customers' needs quickly and efficiently.

This report covers the IT infrastructure supporting the following technology solutions, which are managed by FORTRUST:

- Colocation services
- Remote Hands services

FORTRUST's Data Center and Network Operations and Facilities staff are presently responsible for supporting a variety of customers with the in-scope infrastructure solutions.

Software

Software used by FORTRUST to manage and support FORTRUST's Infrastructure Environment includes:

(1) Nagios for system and network monitoring;
(2) Remote Authentication Dial-In User Service ("RADIUS") for secured access;
(3) Windows Active Directory and security management software for logical and physical access, respectively;
(4) Customer Relationship Management ("CRM") for change management and help desk support software; and
(5) Building Management Software for alarming, monitoring, and management of infrastructure systems.

The FORTRUST IT Environment described herein does not include application software supporting the technology solutions provided by FORTRUST to individual clients or FORTRUST's business unit applications.

People

FORTRUST's organizational structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

FORTRUST employs a staff of approximately 35 people and is supported by the functional areas listed below:

Department	Responsibility
Data Center Operations (including Security)	Day-to-day security of the Data Center, including access administration; assistance; oversight; and customer interface on physical security issues, policies, and procedures.
Facilities	Data Center Facilities configuration, environmental safeguards administration, maintenance, and monitoring and physical configuration/construction of the customer site.
IT Services	Administration, monitoring, and maintenance of the FORTRUST infrastructure and networking components as they relate to the Data Center, including routers and IP assignment and configuration.
Sales and Marketing	Sales and marketing.
Network Operations Center	Remote Hands, Network and Facilities monitoring, ticketing, escalations, receiving, and Data Center Operations oversight. Initiation and oversight of the customer provisioning process.

The managers of each functional area report to the Senior Vice President/General Manager ("SVP/GM"), Senior Vice President ("SVP") of Operations, and/or Chief Executive Officer ("CEO").

All 24x7x365 NOC, Data Center Operations, and Security operational shifts at FORTRUST are managed by the Data Center Operations department. Incident reports, job schedules, and equipment activity are monitored by the Data Center Operations team.

Weekly staff meetings are held to discuss and review tickets, business and operational performance, change management, training, and the management of projects.

References are sought and background checks are conducted for FORTRUST personnel hired. The confidentiality of user entity information is stressed during the new employee orientation program and is emphasized in the Employee Handbook issued to each employee. FORTRUST provides procedures training to all employees and encourages employees to attend external training events.

Procedures

FORTRUST has documented policies and procedures to support the operations and controls over its Data Center managed by FORTRUST's Data Center and Network Operations and Facilities staff. Specific examples of the relevant policies and procedures include the following:

- Policy management and communication
- Physical security administration
- Physical security configuration
- Network availability
- Network device maintenance
- Environmental safeguards
- Incident/problem management
- Customer implementation

Data

FORTRUST does not control customer-specific hardware, operating systems, databases, applications, or any other content loaded on the customers' hardware. FORTRUST does not access customers' systems at the operating system, database, or application levels.

BOUNDARIES OF THE SYSTEM

The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. FORTRUST provides colocation and Remote Hands services to its customers. FORTRUST also provides space, power, and access to its customers. The Company does not have logical access to any customer data and is not responsible for monitoring or supporting customer systems. The boundaries of FORTRUST's System include applications and infrastructure that directly support the colocation services provided to FORTRUST's customers. Any applications and infrastructure that indirectly support the services provided to FORTRUST's customers are not included within the boundaries of FORTRUST's System.

For example, anti-virus settings over FORTRUST's back-office applications and monitoring systems are not within the boundaries of the System, as they do not directly affect FORTRUST's customers, whereas logical security over the monitoring systems and badging system is within the boundaries of the System, as the criteria directly support the service provided to its customers. Similarly, the only back-up activities that are within the boundaries of the System are the network and switch configuration settings, which provide for the availability of network connectivity for its customers. Similarly, as FORTRUST does not have access to customer data, data classification is not within the boundaries of the System.

Additionally, FORTRUST has implemented a disaster recovery and back-up plan that is commensurate with the boundaries and services described above. Redundancy was designed into the infrastructure; therefore, disaster recovery and back-up plans were designed accordingly. FORTRUST's focus on providing redundant power and network connectivity, along with other key areas, provides adequate protection for the infrastructure but may not provide adequate recovery for customer data or hardware. As such, FORTRUST has included the Disaster Recovery Plan in Section Five, "Other Information Provided by FORTRUST that is Not Covered by the Independent Service Auditor's Report," as it is not FORTRUST's responsibility to recover customer systems and data.

The following represents the Trust Services Criteria that are not relevant to the services provided by FORTRUST:

Common Criteria Related to Logical and Physical Access Controls CC5.2 – element related to logical access for customers

New internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.

Common Criteria Related to Logical and Physical Access Controls CC5.3 – element related to logical access for customers

Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).

Common Criteria Related to Logical and Physical Access Controls CC5.7

The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security and availability.

Common Criteria Related to Logical and Physical Access Controls CC5.8

Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.

Availability A.1.3

Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.

PROCESSING ACTIVITIES

Security

FORTRUST has implemented security procedures to prevent and detect unauthorized access to the FORTRUST production network.

Physical Access

FORTRUST maintains security policies that include a section on security awareness. New employees are required to familiarize themselves with the policies for security awareness, sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Company-specific policies and procedures are developed by the CEO, the SVP of Operations, the SVP/GM, and management and communicated to all employees.

Areas designated as controlled secure areas remain secure 24x7x365 and are only accessed by authorized Company personnel and/or visitors and vendors for approved purposes, including maintenance, construction and installation activities, transfer of supplies and equipment, or during emergency situations.

The SVP of Operations is responsible for determining the security access level(s) for all employees. Customer access is granted to customer-designated areas and colocation rooms where their equipment is located based on requests from authorized customer personnel. To obtain access to the customer-designated area and the colocation room, including the customer cages, cabinets, or private rooms, a customer must contact the NOC to request that a particular user be added or removed from the Company's approved list of contacts who have access to the customer-designated areas within the Data Center. This information is maintained in the Premises Access Agreement ("PAA") and in the account file within the CRM ticket management system. The request must be initiated by an authorized customer contact.

Access to the security system software controlling badge readers and biometric scanners to create and delete badges and change access parameters is restricted to authorized personnel.

When an employee voluntarily or involuntarily terminates employment with FORTRUST, Security or other authorized personnel terminate his or her access upon notification. Customer access is removed on a timely basis upon notification, based on requests from authorized customer personnel. Lost or stolen access badges are reported to Security and are immediately deactivated.

The Data Center Operations and NOC personnel are responsible for granting access to vendors and visitors, security reporting procedures, responding to building alarms, and monitoring video surveillance cameras. Internal and external monitoring of Data Center activity is performed through video camera surveillance and alarms, 24x7x365 FORTRUST NOC monitoring, and Data Center walkthroughs performed by NOC personnel multiple times per day.

Customers requiring 24x7x365 access to their cage, cabinet, or private room enter through a separate customer entrance.

Video surveillance cameras are installed throughout the interior and exterior of the Data Center. All video surveillance cameras are positioned to monitor for intrusion activities or possible vulnerabilities and are recorded 24x7x365.

Facility Security

A security badge access system is installed at each facility entrance, which controls access to the Data Center. Each data equipment room housing the customers' cages and cabinets also has badge and fingerprint verification access. The security system, Security Station, and front desk reception maintain logs to record vendor and visitor access into and exiting from the facility, as well as other security events.

Employees, contractors, vendors, and visitors must display a valid access badge to gain entry into the facility. All visitors must sign in at the front desk or Security Station and be escorted. Visitors are required to present a picture ID card, which is shown at the front desk or Security Station before they are issued a temporary ID and permitted into the facility. All personnel must wear and display their FORTRUST identification badges. No individual may knowingly aid another in an attempt to bypass the badge access system or permit access to another individual with the exception of emergency personnel (fire, medical, and police). Personnel must wear a badge at all times while in the facility. There are four types of badges: employee, contractor, customer, and visitor.

Badge Type	Purpose/Access Levels Granted
Employee (Temporary and Permanent)	Issued to the employees of the Data Center. Access is restricted within the Data Center based on employee job responsibility.
Contractor (Temporary and Permanent)	Issued to FORTRUST contractors. Access is granted to areas specific to each contractor's responsibilities.
Customer	Issued to customers and customer representatives upon completion of the PAA form. Only those individuals explicitly listed are issued this badge. Access is granted to customer-designated areas such as the customer staging areas and the customer areas on the Data Center floor.
Visitor	Issued to visitors and vendors performing onsite maintenance, as well as visitors touring the facility; however, this badge type will not allow access through card readers or biometrics.

Customer, employee, and contractor access to critical and sensitive areas (including cages, cabinets, and private rooms) is controlled by multi-level card access and multi-layered biometric authentication devices. The Data Center employs a biometric fingerprint scanning system in addition to badge access as an additional control for customer access identity verification. This system controls access to the customer-designated areas and to private rooms. To gain access, the user scans his or her badge at the terminal and places his or her designated finger on the terminal. The terminal compares the finger on the reader with the user's unique template. If the image matches and the identity is verified, the door is unlocked.

Customer-Designated Area Security

Tumbler locks are used to restrict access to individual customer's cages within the Data Center. A lockbox can be used to secure keys to customer-specific sites, which include cabinets and cages. Each private room housing customers' equipment has badge access and a biometric scanning device. Keys to locked cabinets are restricted to authorized FORTRUST and customer personnel.

When attempting to gain access to the Data Center, a customer must scan his or her badge at the customer entrance or, in some cases, the front business entrance. Customers and vendors must pass through another card reader and enter a security checkpoint at the Security Station. In addition, customers must use the biometric scanning device, which is installed as a secondary form of identification verification.

If a visitor is not pre-authorized for entry, the visitor is prohibited from further access into the Data Center. If the visitor is listed as authorized but has arrived without an access badge, the NOC and/or Security must review the customer's security clearance and determine the cabinet(s), cage(s), or private room to which the customer or vendor is authorized to gain access. Once the NOC and/or Security have determined that the individual has been approved to access the customer's cage, the NOC and/or Security will issue the customer/vendor a visitor badge and provide escorted access to the authorized area.

During normal business hours, if a non-authorized visitor is needed to assist an authorized customer, the visitor must sign in at the front desk or Security Station and receive a visitor's badge. Outside of normal business hours, the customer is requested to make arrangements in advance in order for FORTRUST to allow non-authorized visitors into restricted areas within the Data Center.

Upon leaving the facility, visitors and customers must pass through another card reader and enter the security checkpoint at the Security Station. If a customer does not scan his or her badge prior to entering the security checkpoint, an audible alarm will sound. For escorted access visitors, the visitor is required to return the badge to either the front desk or Security Station and indicate the time leaving the facility.

Environmental Safeguards

To minimize the likelihood of system outages and the effects of failures and disasters on systems and operations, FORTRUST has implemented redundant environmental safeguards and back-up power systems. FORTRUST has established policies and procedures for responding to environmental system failures as well as periodic system maintenance procedures.

The SVP of Operations, SVP/GM, and NOC, as well as Facilities and Security at the Data Center oversee the Data Center environmental safeguards and back-up power management systems. These safeguards and systems include fire suppression, power management, and heating, ventilation, and air conditioning ("HVAC"). FORTRUST also has specific procedures documented for responding to alarm panels, fire alarms, utility power failures, generator failures, Uninterruptible Power Supply ("UPS") system failures, Power Distribution Unit ("PDU") failures, and HVAC failures, as well as periodic system maintenance procedures. Furthermore, FORTRUST has procedures to address imminent shutdowns and restoration of power.

The following describes the environmental safeguards related to FORTRUST's Data Center:

- Air Sampling Fire Detection Early Warning Smoke Detection System
- Dry Pipe, Single Interlocked Pre-Action Fire Suppression System
- Fire extinguishers
- UPS Systems
- Static Transfer Switches ("STS") and PDUs
- Diesel-powered standby generators
- Automatic Transfer Switches ("ATS")
- Environmental Alarm Systems (temperature and humidity)
- Independent HVAC units and central air handling units ("CAHUs")
- Moisture detectors
- Branch Circuit Monitoring (power)

The Data Center is equipped with 36" raised flooring, which is used for uniform cooling and specific distribution of airflow to loads and moisture sensors that monitor for water leakage. No windows or doors in the colocation rooms lead to the exterior of the building.

Fire Detection/Suppression

The Data Center is equipped with smoke detection and fire suppression equipment. Periodic checks and maintenance procedures are performed to test and validate the operation of the fire detection and suppression equipment.

FORTRUST utilizes pre-action dry pipe sprinkler systems for purposes of fire suppression. The system must have two activation events, such as when two smoke detectors detect smoke within the same zone, before water will be deployed into the individual zone. Water will only be released when an individual sprinkler head is fused due to heat. Water will then begin to flow at the location of the activated sprinkler head only. This configuration provides protection against accidental discharge of water by requiring two separate attributes to occur before releasing water. Smoke detectors are mounted on the ceiling and within CAHUs.

In the event of a system malfunction or unnecessary water discharge, the water supply to the sprinkler system can be shut down manually to prevent water damage to the equipment located on the Data Center floor. Additionally, there are fire extinguishers located throughout the Data Center.

Power Management

The Data Center is equipped with a combination of UPS systems and generators in an N+1 configuration to provide continuous power in the event of a power outage. All back-up power systems are capable of maintaining continuous system services to the facility. Periodic checks and maintenance procedures are performed to test and validate the operation of the power management systems.

The Data Center utilizes separate and secure power management and power back-up systems. The Data Center utilizes power from three sources. These include medium voltage 13.2kVA utility feeds, battery-powered UPS systems, and a redundant diesel generator system. The utility power feeds for the Data Center come into the main switchgear room that is located in an environmentally controlled and secure area. The power feeds onsite 2500kVA transformers and then the UPS, which conditions the power and transfers the power to several STS and PDUs located on the Data Center floor. The PDUs distribute the power to the Remote Power Panels that are equipped with Branch Circuit Monitoring for each circuit provided to each cabinet, cage, or private room.

In the event of a brief utility power failure, the UPS instantaneously provides AC power through an inverter from the batteries. In the event of an extended utility power failure, ATS automatically signal the generators to start.

Data Center Operations and Facilities conduct full-load tests utilizing an onsite stationary 3000 amp load bank for each generator every quarter. FORTRUST has multiple source vendors to provide fuel in the event of a prolonged outage at any time of the day.

HVAC

Temperature and humidity are maintained throughout the Data Center through the use of air conditioning, humidity, water detection, and temperature sensors. Periodic checks and maintenance procedures are performed to confirm that HVAC equipment and humidity, temperature, and water detection sensors are working properly.

FORTRUST employs a closed loop propylene glycol chilled water system currently supplied by 440-ton air-cooled chillers and pumps (scalable to 15 chillers and pumps) providing chilled water to the CAHUs in an N+1 configuration to the raised floor area. The raised floor height is 36” and ceiling heights are approximately 18’ and 24’ from slab. Moisture detectors have been installed under the raised floor.

Monitoring

Critical systems and environmental controls are monitored 24x7x365 by the FORTRUST NOC and support staff. Data Center walkthroughs are performed by NOC personnel multiple times per day. The monitoring systems automatically email the team when the temperature and humidity levels go below or above the acceptable threshold, and immediate action is taken on all alarms as they are triggered.

Environmental system issues are documented in the ticket system, escalated, and responded to in accordance with policy timelines. Incident response procedures have been established to notify customers about unexpected events that may impact their systems.

FORTRUST utilizes a Building Management System (“BMS”) to monitor alerts and alarms on environmental, electrical, and fire/life/safety equipment. The BMS has been configured with multiple alarms depending on the severity of the event.

Upon a qualifying event, automated email notifications are sent from the BMS to the Data Center Operations staff, which consists of NOC personnel, Facilities personnel, the SVP/GM, and the SVP of Operations.

The following key environmental and electrical equipment are monitored:

- HVAC – notification occurs when the temperature or humidity reaches pre-determined alarm points.
- PDU/STS/UPS – notification occurs when the preferred power source is not available.

The facility is equipped with an alarm system that triggers an alert when a specific environmental safeguard or power management device is not meeting a certain condition, is not within defined parameters, or is malfunctioning and requires immediate attention, as described above. The alarms are sent to the Operations staff, which consists of NOC personnel. Data Center Operations personnel are notified of the alarm with an email identifying the equipment in the alarm status. The NOC monitors the alarm systems 24x7x365. A CRM ticket is generated for all BMS alarms needing attention and is assigned to the appropriate FORTRUST individual for resolution.

Administrative access to the environmental monitoring systems is restricted to the SVP/GM, SVP of Operations, Critical Systems Manager, and Operations Administrative Assistant.

Certain environmental monitoring and preventive devices are also regularly maintained by their respective vendors.

Network Availability

FORTRUST has established policies and procedures over network availability monitoring, back-ups, maintenance of network devices, and change control.

FORTRUST's infrastructure consists of multiple layers of routers and switches and employs a layered approach to systems security, including perimeter security controls on routers and hardened operating systems. Access is controlled and monitored using defined user authorization processes, authentication, and logging. The Data Center maintains redundant links to the Internet.

Network Operations, in conjunction with the NOC, is responsible for administering and monitoring the logical access to the FORTRUST infrastructure and for ensuring that the services are available. FORTRUST's infrastructure includes the network backbone, consisting of multiple layers of routers and switches. Customers control every aspect of the logical access to their hardware, software, or servers.

The information pulled from the customer's switch port is analyzed and populated into various monitoring systems. The NOC uses various monitoring systems to view alerts. When a failure is detected from a customer port, problem resolution, customer notification, and escalation are conducted in accordance with the appropriate Standard Operating Procedure. Notification emails are sent to the email address(es) the customer has specified for problem notification, which are stored in the CRM and accessible by the NOC.

The NOC is staffed to provide customer support, monitoring, and Remote Hands support 24x7x365. The NOC uses network performance management monitoring tools to monitor all FORTRUST-provided customer switch ports that connect to the Internet. Appropriate FORTRUST personnel are notified of identified problems, CRM tickets are opened, and problems are tracked to resolution. Network availability events must be documented in the ticket system, escalated, and responded to in accordance with policy timelines. Incident response procedures have been established to notify customers about unexpected events that may impact their systems. Procedures have been established and implemented to monitor customer support operations against defined customer service metrics. Management holds weekly staff meetings where open tickets are reviewed and issues are identified and discussed.

Network Device Maintenance

Router Administration

The Data Center contains multiple layers of routers. The routers are administered by Network Operations. Network Operations is responsible for configuring and performing maintenance on all routers.

RADIUS is used to restrict access to all routers from a central location. RADIUS is a security protocol used to provide detailed accounting information and flexible administrative control over authentication and authorization processes. There are redundant RADIUS servers used to administer access to the routers. Access to the RADIUS servers is controlled using Challenge-Handshake Authentication Protocol ("CHAP") or Password Authentication Protocol ("PAP") for authentication. RADIUS is configured so that unique accounts are established for each user through logical groups configured in Active Directory. Network access to routers and switches is provided from authorized FORTRUST IP addresses using password authentication.

Access to the FORTRUST infrastructure is controlled and monitored using defined user authorization processes, authentication, and logging. Logical groups, called Network Access Security ("NAS") groups, have been created on RADIUS to provide access to the routers. Users requiring access to the routers are assigned to user groups, which are in turn assigned to NAS groups. The level of access is assigned at the user group level as either "full" or "read-only." Users assigned to user groups with full access are granted administrative privileges to the routers included in the particular NAS group, whereas users assigned to user groups with read-only access are only allowed to monitor the routers included in the particular NAS group. Administrative access to the network routers and switches is restricted based on job responsibility.

Router Configuration and Maintenance

Each router is configured with Access Control Lists ("ACLs"). ACLs provide security and basic traffic filtering based on source and destination IP address and transmission control protocol and user datagram protocol ports. ACLs are configured to prevent source address spoofing and provide a "perimeter defense" to prevent most known common attacks. ACLs are defined by Network Operations.

Router configuration changes are made by Network Engineers. Typically, configuration changes are made as a result of a new customer installation and the necessity to update the ACLs to include the routing protocols for the new customer. These changes are documented by Network Operations within the account information in the CRM ticket system when requested by the customer. Any configuration changes made to routers are logged and automatically emailed to the Network Engineers and NOC Supervisor and saved in the syslog server.

The following key monitoring systems are used to monitor the network:

- Internap Flow Control Platform System – notification when the Internet Service Provider link is unavailable or the border gateway protocol state has changed.
- Paessler Router Traffic Grapher Internet Bandwidth – notification when abnormal bandwidth usage is identified for more than three minutes.
- Nagios – notification of network links to customers' FORTRUST equipment. Also monitors FORTRUST server uptime and application.

Administrator access to Nagios is controlled through Active Directory. This access is restricted to the SVP/GM, SVP of Operations, NOC Supervisor, System Administrator, IT Manager, and Network Engineers.

Router and switch configuration back-ups are performed daily onto a file server and saved for a minimum of six months. The back-ups are then backed up via a third-party back-up service provider. Note that this back-up service provider is a managed services organization that has been excluded from the scope of this SOC 2 report.

A change management process is followed for any maintenance procedures performed on the routers. The maintenance procedures include both hardware and software/configuration changes. Maintenance procedures are classified as either normal scheduled maintenance, which includes changes not deemed urgent by FORTRUST, or emergency maintenance procedures, which are followed for changes requiring immediate attention.

Normal Scheduled Maintenance

Changes to infrastructure servers or devices are appropriately authorized, documented, and tested and a back-out plan created. Customers are notified whether modifications impact their operations.

Normal scheduled maintenance procedures can occur on Saturdays and Wednesdays from 11:00 p.m. to 5:00 a.m. local time. Normal scheduled maintenance requests must be appropriately documented and approved in accordance with the Change Management Standard Operating Procedure. In addition, Network Operations will create and maintain Maintenance Operation Procedure documents, which document in detail the change being performed, including all pre- and post-change activities, depending on the complexity of the change or maintenance activity to be performed. Once the activity has been defined, it must be approved by the Change Management Board (SVP/GM, SVP of Operations, and IT Services Manager) and be in accordance with the Standard Operating Procedure. When the maintenance is deemed to impact customers, those customers must be notified within 48 hours of the maintenance window prior to work being performed.

Emergency Maintenance

Emergency maintenance procedures may be performed anytime the situation warrants. Emergency maintenance requests require approval from the SVP/GM or the SVP of Operations, in the SVP/GM's absence, and are recommended by the IT Services Manager. When the maintenance is deemed to impact customers, those customers will be notified of the maintenance window as soon as possible and practical prior to work being performed.

Customer Ticketing

FORTRUST has established policies and procedures over customer ticketing to facilitate timely responses to and appropriate tracking of customer and network issues.

The NOC acts as the first level of support for the customers. The NOC consists of several technicians who have been trained to facilitate various types of customer requests. Customers can initiate a request via email or phone. The types of requests include services such as Remote Hands support to reboot a server. The request can also be for connectivity troubleshooting or to update the CRM contact and access list.

If a customer makes a Remote Hands request, the NOC is required to obtain the request in writing from authorized Remote Hands customer personnel. Work is only performed on customer systems as requested by authorized customer representatives over the phone or via email.

The CRM application is used by the NOC for documenting, routing, and tracking customer requests. A CRM ticket is generated for each customer request and is routed to each party involved during the process. If the NOC is unable to address the request, the request is routed to an appropriate member of Network Operations, Facilities, Data Center Operations, and/or management. The NOC communicates with management to ensure that customer requests get resolved in a timely manner. Customer issues and Remote Hands requests are documented in the ticket system, escalated, and responded to in accordance with policy timelines. Customer requests must come from authorized customer personnel. Incident response procedures have been established to notify customers about unexpected events that may impact their systems.

Notice of Event

Telephone

A customer may initiate a request through a 1-866-toll-free number. Calls are handled by the NOC. A CRM ticket is generated and assigned a severity level and priority based on criteria established within the Standard Operating Procedures. An auto-reply is sent to the customer with the CRM ticket number. The NOC has the ability to upgrade or downgrade priority based on the nature of the issue or request.

Email

A customer may initiate a request via email to the NOC email address. Upon sending an email, a CRM ticket is generated and assigned a severity level and priority based on criteria established within the Standard Operating Procedures. An auto-reply is sent to the customer with the CRM ticket number. The NOC has the ability to upgrade or downgrade priority based on the nature of the issue or request.

Administrative access to the CRM application is restricted to the SVP/GM and Network Engineers.

Online

All CRM tickets created via one of the two above methods are owned or assigned by the originator of the ticket. Tickets can be referred out or transferred between the NOC or Network Operations, Facilities, Data Center Operations, or management in order to facilitate seamless routing and escalation of an issue to the proper support organization.

All activity performed for a specific request, including email communication with the customer and work performed, is documented within the CRM ticket. Once a CRM ticket is closed, an email is generated and sent to the customer notifying him or her of the completion of the customer's request.

OTHER ASPECTS OF THE INTERNAL CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS THAT ARE RELEVANT TO THE SERVICES PROVIDED AND THE APPLICABLE TRUST SERVICES CRITERIA

Control Environment

The control environment provides an atmosphere in which people conduct their activities and carry out their control responsibilities. The control environment sets the tone of an organization by influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility; and the way management organizes and develops its people. The objective of the control environment is to establish and promote a collective attitude toward achieving effective internal control over the entity's business.

The control environment has a pervasive influence on the way business activities are structured, objectives are established, and risks are assessed. It also influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive tone at the top. These entities establish appropriate controls, which foster shared values and teamwork in pursuit of an organization's objectives.

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal control over all functional aspects of operations.

Management's philosophy and operating style also affects the way the entity is managed, including the kinds of business risks accepted. FORTRUST places a great deal of importance on working to help ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in the daily operations. Management and specific teams are structured to help ensure the highest level of integrity and efficiency in customer support and transaction processing.

Organizational values, ethics, and behavior standards are communicated through formal job descriptions and through regular departmental meetings and staff interactions. All personnel operate under the FORTRUST personnel policies and procedures, including confidentiality agreements and security policies. Mandatory quarterly compliance training is conducted to communicate regulations and the importance of privacy and security. Management is also committed to being aware of regulatory and economic changes that impact lines of business and continually monitoring the customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management needs to specify the competence levels for particular jobs and translate those levels into requisite knowledge and skills.

FORTRUST management has defined and analyzed the tasks comprising particular jobs, including such factors as the extent to which individuals must exercise judgment and the extent of related supervision. In addition to this, the knowledge and skills required to perform particular jobs have also been determined by management and are communicated to personnel.

Commitment to Competence

Competence of FORTRUST employees is a key element of the control environment. Controls have been developed covering critical aspects of human resources development, including hiring, training and development, advancement, and termination.

FORTRUST is committed to the development of its employees, and this commitment to competence is expressed in the Company's personnel policies. Specific indicators of FORTRUST's commitment to competence and staff development include formal and standardized recruiting and hiring policies and procedures and investment in training and development. Hiring decisions are based on various factors, including educational background, prior relevant experience, past accomplishments, and evidence of integrity and ethical behavior.

Integrity and Ethical Values

Integrity and high ethical standards are qualities essential to the business of FORTRUST and are viewed as fundamental standards of behavior for all employees. At FORTRUST, the standards of integrity and ethics are demonstrated daily by the personal conduct of management and various monitored tone-at-the-top controls, including guidelines for handling confidential information and policies stipulating that employees comply with all laws, regulations, and corporate policies as a condition of continuing employment. FORTRUST has a business conduct and ethics policy outlined in FORTRUST's Employee Handbook and requires all employees to formally acknowledge their commitment to performing in a professional and ethical manner.

Organizational values and behavioral standards are communicated to all personnel through policy statements, an Employee Handbook, and guidelines during new hire orientation and are also available for review on the FORTRUST intranet.

Each employee is expected to report any suspected violation or exception to these policies by another employee of FORTRUST, as well as by vendors, suppliers, and customers. Recognizing the sensitive nature of these situations, employees have several options for bringing these situations to management's attention. FORTRUST has also instituted an open-door policy to facilitate open and frequent communication with management.

Risk Assessment

Risk assessment is the component of the Company's internal control environment that involves identifying and analyzing risks (both internal and external) relevant to achieving business objectives. FORTRUST has placed into operation a risk assessment process to identify and manage risks that could affect FORTRUST's ability to provide reliable service for user entities. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. The process considers both external and internal factors, including economic and industry trends and developments, and entails identifying, prioritizing, and ranking risks at both the entity and activity level. Criteria used to rank risks include, but are not limited to, technological complexity and dependencies and their impact on FORTRUST's services and reputation. This process has identified risks resulting from the nature of the services FORTRUST provides, and management has implemented various measures to manage those risks.

Standard Operating and Contingency Procedures are in place to mitigate the adverse effects of potential negative events. These Standard Operating Procedures provide documentation on operating procedures and standards for various routine, non-critical, and critical functions. Routine and complex maintenance actions are conducted through the use of Maintenance Procedures and Method of Procedure where applicable. FORTRUST also uses Contingency Procedures for processes that are outside the course of normal or routine operations. Documented, validated, and repeatable processes are the cornerstone of FORTRUST's operations. These procedures are revised periodically and distributed to appropriate personnel.

Information and Communication

Information and communication is the component of internal control that ensures pertinent information is identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. They deal with internally generated data, as well as information about external events, activities, and conditions necessary to make informed business decisions. Effective communication also must occur, in a broader sense, throughout the Company. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. Individuals must understand their own role in the internal control system, as well as how individual activities relate to the work of others. Individuals must have a means of communicating significant information upwards within the Company, the objective of which is to ensure that information relevant to operating the business and the maintenance of internal controls and records is identified, captured, and communicated to the appropriate individuals on a timely basis.

Management is committed to maintaining effective communication with all personnel and customers. FORTRUST has implemented policies and procedures to address critical operational processes, including human resources, information systems, and operations.

To ensure alignment of FORTRUST's business strategies and goals with operating performance as it relates to customers, management participates in weekly meetings in order to discuss the status of service delivery or other matters of interest and concern. Issues or suggestions identified by personnel are readily brought to the attention of management to be addressed and resolved.

Monitoring

Monitoring is a process that assesses the quality of the Company's internal control performance over time. Effective monitoring is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations and includes regular management and supervisory activities and other actions personnel take in the performance of their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported throughout the Company with serious matters reported to top management and the board. The objective of monitoring is to detect and remediate control deficiencies throughout the entire system of internal control.

FORTRUST's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. Any exceptions to the quality of internal control performance are discussed during the weekly staff meetings and actions are taken to resolve those exceptions as applicable. FORTRUST employs a variety of "Best in Breed" monitoring systems to collect data for all critical systems, network, and fire/life safety systems throughout the facility and rapidly disseminate the information to support functions throughout the organization.

TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

Although the trust services criteria, and related controls are presented in Section Four, "FORTRUST's Security and Availability Trust Principles and Related Controls and Independent Service Auditor's Description of Tests of Controls and Results of Tests," they are an integral part of FORTRUST's system description.

CHANGES TO THE SYSTEM DURING THE PERIOD

FORTRUST did not have any changes to the System during the period.

COMPLEMENTARY USER ENTITY CONTROLS

FORTRUST's internal control framework was designed with the assumption that specific internal controls would be implemented by user entities. In certain situations, the application of specific internal controls at user entities is necessary to achieve certain trust services criteria included in this report. The user entity's internal controls should be placed in operation to complement FORTRUST's controls. EKS&H LLLP's ("EKS&H") examination was limited to the activities and procedures at FORTRUST as they relate to FORTRUST's user entities. Accordingly, EKS&H's examination did not extend to any activities or procedures in effect at the user entities of FORTRUST. It is each interested party's responsibility to evaluate the complementary user entity's control considerations presented in this section in relation to the internal controls that are in place at user entities to obtain a complete understanding of the internal control system. The portions of the internal controls provided by the user entities and FORTRUST must be evaluated together. If effective user entity internal controls are not in place, FORTRUST's controls may not compensate for such weaknesses.

This section describes other internal controls that should be in operation at user entities to complement the controls at FORTRUST. The auditors of FORTRUST's users should consider whether the following controls have been placed in operation:

Physical Access

User entities are responsible for:

- Communicating to FORTRUST a list of personnel authorized to access their site and periodically reviewing and updating this list to ensure that access remains appropriate.
- Communicating to FORTRUST a list of authorized personnel who can authorize new and changed access to the Data Center and customer-use locations.
- Notifying FORTRUST immediately and in writing whenever the customer desires to terminate the access privileges of any customer employee or other person authorized to have access to the facility or to the customer premises and property, or to terminate or revoke any security access card or key issued as a result of customer authorization.

Network Availability and Network Device Management

User entities are responsible for:

- Responding to DoS notification from FORTRUST within four hours.
- Complying with all laws and regulations with respect to security, availability, maintainability, and integrity.
- Appropriate design and implementation of security architecture at user locations, including firewalls and switch router configuration.
- Restricting access to their infrastructure, hardware, networks, operating systems, applications, databases, and any other content loaded on the hardware at FORTRUST.
- Properly utilizing in a redundant manner a secondary (IP) path ("B" side) provided to the customer's cabinet or rack.

Environmental Safeguards

Power Availability

User entities are responsible for:

- Configuring the "B" side AC power circuit as a "failover" or in a 50% to 50% load-shared configuration; specifically, in a load-shared configuration, the available amperage of one circuit is shared between the "A" side and the "B" side power circuit for (dual power supplies) in a redundant configuration.

Customer Ticketing

Remote Hands

User entities are responsible for:

- Clearly labeling customer equipment.
- Defining the location (cage or cabinet row and rack).
- Specifically describing the request for service.

Customer Implementation

User entities are responsible for:

- Configuring the infrastructure, hardware, network, operating system, application, database, and content.
- Licensing applications that are controlled by them or third parties and are loaded on the servers at FORTRUST.
- Determining their site requirements, including power and connectivity.

General Activities

User entities are responsible for:

- Having appropriate personnel available to report issues and discuss them with FORTRUST personnel.
- Notifying FORTRUST of any changes or updates to their notification information.
- Working with FORTRUST personnel to resolve operational problems.
- Technical support for their equipment at FORTRUST and to their end users.
- Configuring, administering, monitoring, and repairing all software and hardware failures.
- Communicating to FORTRUST a list of employees authorized to initiate a Remote Hands request.
- Providing written or real-time instructions for shut-down and rebooting the System/hardware requests.
- Installation and maintenance of virus protection software on the systems at FORTRUST.
- Complying with all laws and regulations with respect to security, availability, maintainability, and integrity.

The list of complementary user entity control considerations presented above is not and should not be considered a comprehensive list of all internal controls that should be employed by the users of FORTRUST. Other internal controls may be required at user entities.

SECTION FOUR

FORTRUST'S SECURITY AND AVAILABILITY TRUST PRINCIPLES AND RELATED CONTROLS AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS OF TESTS

FORTRUST'S SECURITY AND AVAILABILITY TRUST *PRINCIPLES* AND RELATED CONTROLS AND INDEPENDENT SERVICE AUDITOR'S TESTS OF CONTROLS AND RESULTS OF TESTS

Introduction

This examination was conducted in accordance with the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2 ®).*

This section presents the following information provided by FORTRUST:

- The relevant trust services criteria and the controls established and specified by FORTRUST to meet the relevant security and availability trust services criteria to support that:
    - Security: The system is protected against unauthorized access, use, or modification.
    - Availability: The system is available for operation and use as committed or agreed.

Although the relevant security and availability trust services criteria and related controls are presented in Section Four, they are an integral part of FORTRUST's Description of its System.

Also included in this section is the following information provided by the independent service auditor, EKS&H:

- A description of the testing performed by EKS&H to determine whether FORTRUST's controls were operating with sufficient effectiveness to achieve the relevant security and availability trust services criteria. EKS&H determined the nature, timing, and extent of the testing performed; and
- The results of EKS&H's tests of operating effectiveness.

1.0 Common Criteria Related to Organization and Management			
Organization and Management Common Criteria 1.1 Description The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.1.1	FORTRUST has written organization charts based on reporting lines and authorities.	**Inquiry and Inspection** Inquired of management and inspected the FORTRUST organization charts to determine whether they are based on reporting lines and authorities.	No deviations noted.
CC1.1.2	FORTRUST maintains security policies that address both IT and physical security and availability policies that address the availability of the system. Policies and procedures are required to be periodically reviewed and approved by either the SVP of Operations or SVP/GM. The SVP of Operations is responsible for the system availability and related security policies.	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's policies to determine whether security policies were in place that address both IT and physical security for the in-scope technology and whether availability policies were in place that address the availability of the system. **Inquiry and Inspection** Inquired of management to determine whether the SVP of Operations is responsible for the system availability and related security policies. For a selection of security and availability policies that were updated during the audit period, inspected documentation to determine whether the policies were reviewed and approved by either the SVP of Operations or SVP/GM. **Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted. No deviations noted. No deviations noted.

1.0 Common Criteria Related to Organization and Management			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.1.3	FORTRUST has in place a formal and comprehensive compilation of documented policies. All policies are assigned responsibility to appropriate management and are updated as changes occur and reviewed for appropriate updates at a minimum of an annual basis. They are centrally stored and accessible to all appropriate personnel for regular review. Policies cover the following areas: • Purpose • Policy Statement • Goals and Objectives • Roles and Responsibilities • All positions • Applicability • Authority • Revision History	**Inquiry** Inquired of management to determine whether FORTRUST has formal documented policies, and whether all policies are assigned responsibility to appropriate management, are updated as changes occur, are reviewed for appropriate updates at a minimum of an annual basis, and are centrally stored and accessible to all appropriate personnel for regular review. **Inspection** Inspected FORTRUST's IT security policies and procedures to determine whether policies and procedures over system security and availability are established and periodically reviewed and approved by management.	No deviations noted. No deviations noted.
CC1.1.4	FORTRUST has written job descriptions specifying the roles and responsibilities for key job positions.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected job descriptions to determine whether the roles and responsibilities for key job positions.	No deviations noted.

1.0 Common Criteria Related to Organization and Management			
Organization and Management Common Criteria 1.2 Description Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and placed in operation.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.2.1	FORTRUST maintains security policies that address both IT and physical security and availability policies that address the availability of the system. Policies and procedures are required to be periodically reviewed and approved by either the SVP of Operations or SVP/GM. The SVP of Operations is responsible for the system availability and related security policies.	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's policies to determine whether security policies were in place that address both IT and physical security for the in-scope technology and whether availability policies were in place that address the availability of the system.	No deviations noted.
		Inquiry and Inspection Inquired of management to determine whether the SVP of Operations is responsible for the system availability and related security policies. For a selection of security and availability policies that were updated during the audit period, inspected documentation to determine whether the policies were reviewed and approved by either the SVP of Operations or SVP/GM.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted.
Organization and Management Common Criteria 1.3 Description Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability have the qualifications and resources to fulfill their responsibilities.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.3.1	Employee performance evaluations support the achievement of security and availability objectives.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected performance evaluations to determine whether evaluations are performed to support the achievement of security and availability objectives.	No deviations noted.

1.0 Common Criteria Related to Organization and Management			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.3.2	Management supports employees by providing tools and training needed to perform their security and availability related roles.	**Inquiry** Inquired of management to determine whether management supports employees by providing tools and training needed to perform their security and availability related roles.	No deviations noted.
		Inspection For a selection of policies and procedures changed during the period, inspected the policy tracking sheet to determine that employees acknowledged their agreement to the changed policy or procedure.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted.
CC1.3.3	FORTRUST performs background checks appropriate to the role and prior to hire. Multiple levels of interviews are performed prior to hire to evaluate the candidate's ability to meet FORTRUST's requirements and perform the job duties.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected background checks to determine whether background checks are appropriate to the role and prior to hire and that multiple levels of interviews are performed prior to hire to evaluate the candidate's ability to meet FORTRUST's requirements and perform the job duties.	No deviations noted.
CC1.3.4	FORTRUST has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected job descriptions to determine whether the descriptions specified the responsibilities and academic and professional requirements for the job positions.	No deviations noted.

1.0 Common Criteria Related to Organization and Management			
Organization and Management Common Criteria 1.4 Description The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.4.1	Employee performance evaluations support the achievement of security and availability objectives.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected performance evaluations to determine whether evaluations are performed to support the achievement of security and availability objectives.	No deviations noted.
CC1.4.2	Management supports employees by providing tools and training needed to perform their security and availability related roles.	**Inquiry** Inquired of management to determine whether management supports employees by providing tools and training needed to perform their security and availability related roles. **Inspection** For a selection of policies and procedures changed during the period, inspected the policy tracking sheet to determine that employees acknowledged their agreement to the changed policy or procedure. **Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted. No deviations noted. No deviations noted
CC1.4.3	FORTRUST has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected job descriptions to determine whether the descriptions specified the responsibilities and academic and professional requirements for the job positions.	No deviations noted.

1.0 Common Criteria Related to Organization and Management			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC1.4.4	New employees are required to familiarize themselves with the policies over security awareness and sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Changes to system boundaries or to policies and procedures are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change.	**Inquiry and Inspection** Inquired of management and for a selection of new employees, inspected employee acknowledgements to determine whether new employees familiarize themselves with the policies over security awareness and receive site-specific security orientation. For a selection of existing employees, inspected acknowledgements to deter ermine whether existing employees acknowledge the Employee Handbook on an annual basis**.** **Inquiry** Inquired of management to determine whether changes to system boundaries or to policies and procedures are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change.	No deviations noted. No deviations noted.
CC1.4.5	FORTRUST performs background checks appropriate to the role and prior to hire. Multiple levels of interviews are performed prior to hire to evaluate the candidate's ability to meet FORTRUST's requirements and perform the job duties.	**Inquiry and Inspection** Inquired of management and for a selection of employees, inspected background checks to determine whether background checks are appropriate to the role and prior to hire and that multiple levels of interviews are performed prior to hire to evaluate the candidate's ability to meet FORTRUST's requirements and perform the job duties.	No deviations noted.

2.0 Common Criteria Related to Communications			
Communications Common Criteria 2.1 Description Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.1.1	FORTRUST has prepared a description of the system, its boundaries, and processes that includes infrastructure, software, people, procedures, and data and communicates such descriptions and clients' security and availability commitments and obligations to clients through electronic means and customer guides. This description includes the process for informing the entity about breaches of system security and submitting complaints.	**Inquiry and Inspection** Corroborated with management and inspected FORTRUST's website and Master Services Agreements to determine whether management communicates boundaries and obligations and whether the description addresses infrastructure, software, people, procedures, and data for the in-scope technology and includes a process for informing the entity about breaches and complaints. **Inspection** For a selection of new customers, inspected the completed Customer Operations Reference Guide and Master Service Agreement to determine whether the security and availability obligations of the users and FORTRUST's security and availability commitments are acknowledged and communicated to authorized users.	No deviations noted. No deviations noted.

2.0 Common Criteria Related to Communications			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.1.2	New employees are required to familiarize themselves with the policies over security awareness and sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Changes to system boundaries or to policies and procedures around security, availability, and breaches are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change.	**Inquiry and Inspection** Corroborated with management and for a selection of new employees, inspected corresponding employee acknowledgements to determine whether they acknowledged their understanding and willingness to comply with FORTRUST policies and receipt of site specific security orientation. **Inquiry and Inspection** Corroborated with management and for a selection of existing employees, inspected corresponding employee acknowledgements to determine whether they acknowledged the Employee Handbook during the audit period. **Inquiry and Inspection** Corroborated with management and for a selection of changes to system boundaries and policies and procedures during the audit period, obtained and inspected evidence to determine whether employees acknowledged their receipt and understanding of the changes.	No deviations noted. No deviations noted. No deviations noted.
Communications Common Criteria 2.2 Description The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.2.1	FORTRUST has prepared a description of the system, its boundaries, and processes that includes infrastructure, software, people, procedures, and data and communicates such descriptions and clients' security and availability commitments and obligations to clients through electronic means and customer guides.	**Inquiry and Inspection** Corroborated with management and inspected FORTRUST's website and Master Services Agreements to determine whether management communicates boundaries and obligations and whether the description addresses infrastructure, software, people, procedures, and data for the in-scope technology. **Inspection** For a selection of customers, inspected the completed Customer Operations Reference Guide to determine whether the security and availability obligations of the users and FORTRUST's security and availability commitments are communicated to authorized users**.**	No deviations noted. No deviations noted.

2.0 Common Criteria Related to Communications			
Communications Common Criteria 2.3 Description The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.3.1	New employees are required to familiarize themselves with the policies over security awareness and sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Changes to system boundaries or to policies and procedures around security, availability, and breaches are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change. Management holds weekly staff meetings where open tickets are reviewed, issues are identified and discussed, and changes that may affect system security and availability are communicated to managers and users who could be affected. FORTRUST has prepared a description of the system, its boundaries, and processes that includes infrastructure, software, people, procedures, and data and communicates such descriptions and clients' security and availability commitments and obligations to clients through electronic means and customer guides. This description includes the process for informing the entity about breaches of system security and submitting complaints.	**Inquiry and Inspection** Corroborated with management and for a selection of new employees, inspected corresponding employee acknowledgements to determine whether they acknowledged their understanding and willingness to comply with FORTRUST policies and receipt of site specific security orientation. **Inquiry and Inspection** Corroborated with management and for a selection of existing employees, inspected corresponding employee acknowledgements to determine whether they acknowledged the Employee Handbook during the audit period. **Inquiry and Inspection** Corroborated with management and for a selection of changes to system boundaries and policies and procedures during the audit period, obtained and inspected evidence to determine whether employees acknowledged their receipt and understanding of the changes.	No deviations noted. No deviations noted. No deviations noted.

2.0 Common Criteria Related to Communications			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.3.2	FORTRUST has prepared a description of the system, its boundaries, and processes that includes infrastructure, software, people, procedures, and data and communicates such descriptions and clients' security and availability commitments and obligations to clients through electronic means and customer guides.	**Inquiry and Inspection** Corroborated with management and inspected FORTRUST's website and Master Services Agreements to determine whether management communicates boundaries and obligations and whether the description addresses infrastructure, software, people, procedures, and data for the in-scope technology. **Inspection** For a selection of customers, inspected the completed Customer Operations Reference Guide to determine whether the security and availability obligations of the users and FORTRUST's security and availability commitments are communicated to authorized users.	No deviations noted. No deviations noted.
CC2.3.3	FORTRUST holds weekly staff meetings where responsibility and accountability for its system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	**Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes and updates to system security and availability policies were discussed with personnel responsible for implementing them.	No deviations noted.

2.0 Common Criteria Related to Communications			
Communications Common Criteria 2.4 Description Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls relevant to the security and availability of the system have the information necessary to carry out those responsibilities.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.4.1	FORTRUST's security and availability policies and procedures address the following: a. Organization and management b. Communications c. Risk management d. Monitoring e. Logical and physical access f. System operations g. Change management h. System recovery and business continuity i. Monitoring system capacity	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's IT security and availability policies and procedure documents to determine whether FORTRUST's security and availability policies address the criteria noted in the control description.	No deviations noted.

2.0 Common Criteria Related to Communications			
Communications Common Criteria 2.5 Description Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.5.1	FORTRUST has prepared a description of the system, its boundaries, and processes that includes infrastructure, software, people, procedures, and data and communicates such descriptions and clients' security and availability commitments and obligations to clients through electronic means and customer guides. This description includes the process for informing the entity about breaches of system security and submitting complaints.	**Inquiry and Inspection** Corroborated with management and inspected FORTRUST's website and Master Services Agreements to determine whether management communicates Boundaries and obligations and whether the description addresses infrastructure, software, people, procedures, and data for the in-scope technology and includes a process for informing the entity about breaches and complaints. **Inspection** For a selection of new customers, inspected the completed Customer Operations Reference Guide and Master Service Agreement to determine whether the security and availability obligations of the users and FORTRUST's security and availability commitments are acknowledged and communicated to authorized users.	No deviations noted. No deviations noted.

2.0 Common Criteria Related to Communications			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.5.2	New employees are required to familiarize themselves with the policies over security awareness and sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Changes to system boundaries or to policies and procedures around security, availability, and breaches are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change.	**Inquiry and Inspection** Corroborated with management and for a selection of new employees, inspected corresponding employee acknowledgements to determine whether they acknowledged their understanding and willingness to comply with the FORTRUST policies and receipt of site specific security orientation.	No deviations noted.
		Inquiry and Inspection Corroborated with management and for a selection of existing employees, inspected corresponding employee acknowledgements to determine whether they acknowledged the Employee Handbook during the audit period.	No deviations noted.
		Inquiry and Inspection Corroborated with management and for a selection of changes to system boundaries and policies and procedures during the audit period, obtained and inspected evidence to determine whether employees acknowledged their receipt and understanding of the changes.	No deviations noted.
CC2.5.3	Authorized customers, via the Customer Operations Reference Guide ("CORG"), are instructed on submitting complaints and who to contact if they become aware of a possible security breach.	**Inquiry and Inspection** Corroborated with management and for a selection of customers, inspected the related CORG form for user entities to determine whether authorized customers were instructed on submitting complaints and who to contact if they become aware of a possible security breach.	No deviations noted.

2.0 Common Criteria Related to Communications			
Communications Common Criteria 2.6 Description System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC2.6.1	Procedures have been established and implemented to monitor customer support operations against defined customer service metrics. Management holds weekly staff meetings where open tickets are reviewed, issues are identified and discussed, and changes that may affect system security and availability are communicated to managers and users who could be affected.	**Inquiry** Inquired of management to determine whether procedures have been established and implemented to monitor customer support operations against defined customer service metrics. **Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether open tickets were reviewed and whether issues were identified and discussed. **Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security and availability are communicated to managers and users who could be affected.	No deviations noted. No deviations noted. No deviations noted.
CC2.6.2	Changes to infrastructure servers or devices are authorized, documented, and tested and a back-out plan created. Customers are notified whether modifications impact their operations.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets for changes to infrastructure servers and devices to determine whether the changes were authorized, documented, tested, back-out plans were documented, and that customers affected by the changes were notified.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
Risk Management and Design and Implementation of Controls Common Criteria 3.1 Description The entity (1) identifies potential threats that would impair system security and availability commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.1.1	The NOC is staffed to provide customer support, monitoring, and Remote Hands support 24x7x365. The NOC uses network performance management monitoring tools to monitor all FORTRUST provided customer switch ports that connect to the Internet. Appropriate FORTRUST personnel are notified of identified problems, CRM tickets are opened, and problems are tracked to resolution.	**Observation** At multiple times during the audit period, observed the NOC utilize network performance management monitoring tools to monitor network performance.	No deviations noted.
		Inspection For a selection of days, inspected email notifications and walkthrough checklists to determine whether NOC personnel documented the performance of 24x7x365 monitoring as well as walkthroughs of the Data Center multiple times per day.	No deviations noted.
		Inspection Inspected email configuration settings within the syslog and network performance monitoring tools to determine whether FORTRUST personnel are automatically notified of identified problems. Inspected an example email to determine whether the email was sent based on the configuration.	No deviations noted.
		Observation Observed the configuration settings within the monitoring systems and the corresponding email to determine whether FORTRUST personnel are notified when the temperature and humidity levels go below an acceptable threshold.	No deviations noted.
		Inquiry and Observation Inquired of management and observed the monitoring system user listing to determine whether access is restricted to authorized FORTRUST personnel.	No deviations noted.
		Inspection Inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.1.2	FORTRUST maintains a risk assessment and threat analysis for risks against the system. When high severity incidents or breaches are identified, a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. The risk assessment is updated annually or as needed based on significant events.	**Inquiry** Inquired of management to determine whether FORTRUST maintains a risk assessment and threat analysis for risks against the system. When high severity incidents or breaches are identified, a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. The risk assessment is updated annually or as needed based on significant events.	No deviations noted.
		Inspection For a selection of high severity tickets/breaches, inquired of management and inspected the risk assessment to determine whether a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution.	No deviations noted.
		Inspection Inspected the risk assessment to determine whether the assessment is updated on an annual basis or as needed based on significant events.	No deviations noted.
CC3.1.3	Customer issues, internal issues, and Remote Hands requests are documented in the ticket system, escalated, and responded to in accordance with policy timelines. Customer requests must come from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of tickets and premises authorization forms to determine whether customer-requested issues were authorized by approved customer personnel.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.1.4	Incident response procedures have been established to notify customers about unexpected events that may impact their systems.	**Inquiry** Inquired of management and inspected incident response procedures to determine whether incident response procedures have been established to notify customers about unexpected events that may impact their systems. **Inspection** Inspected a selection of tickets to determine whether customers were notified of incidents impacting their operations.	No deviations noted. Circumstances that warrant the operation of this control did not occur during the period; therefore, no testing was performed.
CC3.1.5	Procedures have been established and implemented to monitor customer support operations against defined customer service metrics. Management holds weekly staff meetings where open tickets are reviewed, issues are identified and discussed, and changes that may affect system security and availability are communicated to managers and users who could be affected.	**Inquiry** Inquired of management to determine whether procedures have been established and implemented to monitor customer support operations against defined customer service metrics. **Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether open tickets were reviewed and whether issues were identified and discussed. **Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security and availability are communicated to managers and users who could be affected.	No deviations noted. No deviations noted. No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
Risk Management and Design and Implementation of Controls Common Criteria 3.2 Description The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.2.1	FORTRUST maintains security policies that address both IT and physical security and availability policies that address the availability of the system. Policies and procedures are required to be periodically reviewed and approved by either the SVP of Operations or SVP/GM. The SVP of Operations is responsible for the system availability and related security policies.	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's policies to determine whether security policies were in place that address both IT and physical security for the in-scope technology and whether availability policies were in place that address the availability of the system.	No deviations noted.
		Inquiry and Inspection Inquired of management to determine whether the SVP of Operations is responsible for the system availability and related security policies. For a selection of security and availability policies that were updated during the audit period, inspected documentation to determine whether the policies were reviewed and approved by either the SVP of Operations or SVP/GM.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.2.2	FORTRUST's security and availability policies and procedures address the following: a. Organization and management b. Communications c. Risk management d. Monitoring e. Logical and physical access f. System operations g. Change management h. System recovery and business continuity i. Monitoring system capacity	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's IT security and availability policies and procedure documents to determine whether FORTRUST's security and availability policies address the criteria noted in the control description.	No deviations noted.
CC3.2.3	FORTRUST holds weekly staff meetings where responsibility and accountability for its system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	**Inquiry and Inspection** Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes and updates to system security and availability policies were discussed with personnel responsible for implementing them.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.2.4	FORTRUST maintains security policies that address both IT and physical security and availability policies that address the availability of the system. Policies and procedures are required to be periodically reviewed and approved by either the SVP of Operations or SVP/GM. The SVP of Operations is responsible for the system availability and related security policies.	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's policies to determine whether security policies were in place that address both IT and physical security for the in-scope technology and whether availability policies were in place that address the availability of the system.	No deviations noted.
		Inquiry and Inspection Inquired of management to determine whether the SVP of Operations is responsible for the system availability and related security policies. For a selection of security and availability policies that were updated during the audit period, inspected documentation to determine whether the policies were reviewed and approved by either the SVP of Operations or SVP/GM.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.2.5	New employees are required to familiarize themselves with the policies over security awareness and sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Changes to system boundaries or to policies and procedures around security, availability, and breaches are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change.	**Inquiry and Inspection** Corroborated with management and for a selection of new employees, inspected corresponding employee acknowledgements to determine whether they acknowledged their understanding and willingness to comply with FORTRUST policies and receipt of site specific security orientation.	No deviations noted.
		Inquiry and Inspection Corroborated with management and for a selection of existing employees, inspected corresponding employee acknowledgements to determine whether they acknowledged the Employee Handbook during the audit period.	No deviations noted.
		Inquiry and Inspection Corroborated with management and for a selection of changes to system boundaries and policies and procedures during the audit period, obtained and inspected evidence to determine whether employees acknowledged their receipt and understanding of the changes.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
Risk Management and Design and Implementation of Controls Common Criteria 3.3 Description The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security and availability and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.3.1	Procedures have been established and implemented to monitor customer support operations against defined customer service metrics. Management holds weekly staff meetings where open tickets are reviewed, issues are identified and discussed, and changes that may affect system security and availability are communicated to managers and users who could be affected.	**Inquiry** Inquired of management to determine whether procedures have been established and implemented to monitor customer support operations against defined customer service metrics.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether open tickets were reviewed and whether issues were identified and discussed.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security and availability are communicated to managers and users who could be affected.	No deviations noted.

3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC3.3.2	FORTRUST maintains a risk assessment and threat analysis for risks against the system. When high severity incidents or breaches are identified, a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. The risk assessment is updated annually or as needed based on significant events.	**Inquiry** Inquired of management to determine whether FORTRUST maintains a risk assessment and threat analysis for risks against the system. When high severity incidents or breaches are identified, a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. The risk assessment is updated annually or as needed based on significant events.	No deviations noted.
		Inspection For a selection of high severity tickets/breaches, inquired of management and inspected the risk assessment to determine whether a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution.	No deviations noted.
		Inspection Inspected the risk assessment to determine whether the assessment is updated on an annual basis or as needed based on significant events.	No deviations noted.
CC3.3.3	New employees are required to familiarize themselves with the policies over security awareness and sign an acknowledgement of their understanding and willingness to comply with these policies, and receive site-specific security orientation. Existing employees are required to acknowledge the Employee Handbook on an annual basis. Changes to system boundaries or to policies and procedures around security, availability, and breaches are communicated to employees who are required to read the changed policy or procedure and sign their acknowledgment of having read the change.	**Inquiry and Inspection** Corroborated with management and for a selection of new employees, inspected corresponding employee acknowledgements to determine whether they acknowledged their understanding and willingness to comply with FORTRUST policies and receipt of site specific security orientation.	No deviations noted.
		Inquiry and Inspection Corroborated with management and for a selection of existing employees, inspected corresponding employee acknowledgements to determine whether they acknowledged the Employee Handbook during the audit period.	No deviations noted.
		Inquiry and Inspection Corroborated with management and for a selection of changes to system boundaries and policies and procedures during the audit period, obtained and inspected evidence to determine whether employees acknowledged their receipt and understanding of the changes.	No deviations noted.

4.0 Common Criteria Related to Monitoring of Controls			
Monitoring of Controls Common Criteria 4.1 Description The design and operating effectiveness of controls are periodically evaluated against security and availability commitments and requirements, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC4.1.1	The NOC is staffed to provide customer support, monitoring, and Remote Hands support 24x7x365. The NOC uses network performance management monitoring tools to monitor all FORTRUST provided customer switch ports that connect to the Internet. Appropriate FORTRUST personnel are notified of identified problems, CRM tickets are opened, and problems are tracked to resolution.	**Observation** At multiple times during the audit period, observed the NOC utilize network performance management monitoring tools to monitor network performance.	No deviations noted.
		Inspection For a selection of days, inspected email notifications and walkthrough checklists to determine whether NOC personnel documented the performance of 24x7x365 monitoring as well as walkthroughs of the Data Center multiple times per day.	No deviations noted.
		Inspection Inspected email configuration settings within the syslog and network performance monitoring tools to determine whether FORTRUST personnel are automatically notified of identified problems. Inspected an example email to determine whether the email was sent based on the configuration.	No deviations noted.
		Observation Observed the configuration settings within the monitoring systems and the corresponding email to determine whether FORTRUST personnel are notified when the temperature and humidity levels go below an acceptable threshold.	No deviations noted.
		Inquiry and Observation Inquired of management and observed the monitoring system user listing to determine whether access is restricted to authorized FORTRUST personnel.	No deviations noted.
		Inspection Inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.

4.0 Common Criteria Related to Monitoring of Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC4.1.2	Network availability events must be documented in the ticket system, escalated, and responded to in accordance with policy timelines.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets to determine whether network availability events were documented in the ticket system, escalated, and responded to in accordance with policy timelines.	No deviations noted.
CC4.1.3	Customer issues, internal issues, and Remote Hands requests are documented in the ticket system, escalated, and responded to in accordance with policy timelines. Customer requests must come from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of tickets and premises authorization forms to determine whether customer requested issues were authorized by approved customer personnel.	No deviations noted.
CC4.1.4	Management holds weekly staff meetings where open tickets are reviewed, issues are identified and discussed, and changes that may affect system security and availability are communicated to managers and users who could be affected.	**Inquiry** Inquired of management to determine whether procedures have been established and implemented to monitor customer support operations against defined customer service metrics.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether open tickets were reviewed and whether issues were identified and discussed.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security and availability are communicated to managers and users who could be affected.	No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
Logical and Physical Access Controls Common Criteria 5.1 Description Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.1.1	Access to the security system software controlling badge readers and biometric scanners to create and delete badges and change access parameters is limited to NOC personnel, the SVP/GM, VP of Operations, Facilities Manager, and Data Center Operations personnel.	**Inquiry and Inspection** Inquired of management and inspected the security system software user listing to determine whether access to create and delete badges and change access parameters is restricted to authorized personnel.	No deviations noted.
CC5.1.2	Administrative access to the network routers and switches is restricted based on job responsibility.	**Inquiry and Inspection** Inquired of management and inspected user access listings within Active Directory, which controls access to all FORTRUST infrastructure, to determine whether administrative access is restricted based on job responsibility.	No deviations noted.
CC5.1.3	Administrator access to the network and infrastructure monitoring tool, Nagios, is controlled through Active Directory. This access is restricted to the SVP/GM, VP of Operations, NOC Supervisor, System Administrator, Facilities and IT Managers, and Network Engineers.	**Inquiry and Inspection** Inquired of management and inspected the Domain Administrators in Active Directory to determine whether administrative access to Nagios is restricted to the SVP/GM, VP of Operations, NOC Supervisor, System Administrator, Facilities and IT Managers, and Network Engineers.	No deviations noted.
CC5.1.4	Any configuration changes made to routers are logged and automatically emailed to the Network Engineers and NOC Supervisor and saved on the syslog server.	**Inquiry and Inspection** Inquired of management and for a selection of routers, inspected system configurations to confirm that all routers are configured to notify the Network Engineers and NOC Supervisor of any changes. **Inspection** For a selection of routers, inspected a sample notification sent when a configuration change is made to the router to determine whether it was emailed as configured.	No deviations noted. No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
Logical and Physical Access Controls Common Criteria 5.2 Description New internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.2.1	Network access to routers and switches is provided from authorized FORTRUST IP addresses, using password authentication.	**Inquiry and Inspection** Inquired of management and inspected Active Directory password settings that control network access to routers and switches to determine whether passwords require a minimum length, are complex, and are required to change frequently. **Inspection** For a selection of routers, inspected the ACL settings to determine whether access is restricted to FORTRUST IP addresses, denying all others.	No deviations noted. No deviations noted.
CC5.2.2	Administrative access to the network routers and switches is restricted based on job responsibility.	**Inquiry and Inspection** Inquired of management and inspected user access listings within Active Directory, which controls access to all FORTRUST infrastructure, to determine whether administrative access is restricted based on job responsibility.	No deviations noted.
CC5.2.3	Access to the security system software controlling badge readers and biometric scanners to create and delete badges and change access parameters is limited to NOC personnel, the SVP/GM, VP of Operations, Facilities Manager, and Data Center Operations personnel.	**Inquiry and Inspection** Inquired of management and inspected the security system software user listing to determine whether access to create and delete badges and change access parameters is restricted to authorized personnel.	No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.2.4	When an employee voluntarily or involuntarily terminates employment with FORTRUST, Data Center Operations Security personnel or other authorized personnel terminate his or her access upon notification. Customer access is disabled through a password change on their account on a timely basis upon notification based on requests from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of terminated employees to determine whether Data Center badge access was removed timely and Active Directory passwords were changed in a timely manner. **Inspection** Inspected a selection of customer and contractor requests to remove badge access to determine whether access was requested by authorized customer personnel and whether access was removed in a timely manner.	No deviations noted. No deviations noted.
The element of this criterion related to logical access for customers is not applicable to the services provided by FORTRUST.			
Logical and Physical Access Controls Common Criteria 5.3 Description Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.3.1	Network access to routers and switches is provided from authorized FORTRUST IP addresses, using password authentication.	**Inquiry and Inspection** Inquired of management and inspected Active Directory password settings that control network access to routers and switches to determine whether passwords require a minimum length, are complex, and are required to change frequently. **Inspection** For a selection of routers, inspected the ACL settings to determine whether access is restricted to FORTRUST IP addresses, denying all others.	No deviations noted. No deviations noted.
The element of this criterion related to logical access for customers is not applicable to the services provided by FORTRUST.			

5.0 Common Criteria Related to Logical and Physical Access Controls			
Logical and Physical Access Controls Common Criteria 5.4 Description Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.4.1	Network access to routers and switches is provided from authorized FORTRUST IP addresses, using password authentication.	**Inquiry and Inspection** Inquired of management and inspected Active Directory password settings that control network access to routers and switches to determine whether passwords require a minimum length, are complex, and are required to change frequently. **Inspection** For a selection of routers, inspected the ACL settings to determine whether access is restricted to FORTRUST IP addresses, denying all others.	No deviations noted. No deviations noted.
CC5.4.2	Administrative access to the network routers and switches is restricted based on job responsibility.	**Inquiry and Inspection** Inquired of management and inspected user access listings within Active Directory, which controls access to all FORTRUST infrastructure, to determine whether administrative access is restricted based on job responsibility.	No deviations noted.
Logical and Physical Access Controls Common Criteria 5.5 Description Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.5.1	The Data Center VP of Operations is responsible for determining security access level(s) for all FORTRUST employees. The VP of Operations, SVP/GM, or Facilities Manager is responsible for determining security access levels for contractors. Customer access is granted to customer-designated areas and co-location rooms where their equipment is located based on requests from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of help desk tickets that included customers, employees, and contractors granted physical access to the Data Center and customer-use locations to determine whether access was provided based on requests from authorized customer personnel and/or approved by the VP of Operations and access was restricted to only the locations where the equipment is located.	No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.5.2	When an employee voluntarily or involuntarily terminates employment with FORTRUST, Data Center Operations Security personnel or other authorized personnel terminate his or her access upon notification. Customer access is disabled through a password change on their account on a timely basis upon notification based on requests from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of terminated employees to determine whether Data Center badge access was removed timely and Active Directory passwords were changed in a timely manner. **Inspection** Inspected a selection of customer and contractor requests to remove badge access to determine whether access was requested by authorized customer personnel and whether access was removed in a timely manner.	No deviations noted. No deviations noted.
CC5.5.3	Internal and external monitoring of Data Center activity is performed through video camera surveillance and alarms, 24x7x365 FORTRUST NOC monitoring, and Data Center walkthroughs performed by NOC personnel multiple times per day.	**Inquiry and Inspection** Inquired of management and inspected internal and external security monitoring procedures over the Data Center and the NOC. **Observation** Observed video camera surveillance and alarms to determine whether internal and external monitoring of Data Center activity is performed. **Observation** Observed the NOC monitoring over physical security. **Inspection** For a selection of days, inspected email notifications and walkthrough checklists to determine whether NOC personnel documented the performance of 24x7x365 monitoring as well as walkthroughs of the Data Center multiple times per day.	No deviations noted. No deviations noted. No deviations noted. No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.5.4	All visitors must sign in at the front desk or Security Station and be escorted through the facility. Visitors are required to present a picture ID card, which is shown at the front desk or Security Station before they are issued a temporary ID and permitted into the facility. All personnel must wear and display their FORTRUST ID badges.	**Inquiry and Inspection** Inquired of management and inspected policies and procedures to determine whether visitors are required to present picture ID. **Observation** Observed visitors sign in at the front desk, present picture IDs, and be escorted throughout the facility. **Observation** Observed personnel wearing and displaying their FORTRUST ID badges.	No deviations noted. No deviations noted. No deviations noted.
CC5.5.5	Customer, employee, and contractor access to critical and sensitive areas (including cages, cabinets, and private rooms) is controlled by multi-level card access and multi-layered biometric authentication devices.	**Inquiry and Observation** Inquired of management and observed critical and sensitive areas to determine whether access is controlled by multi-level card access and biometric authentication devices. **Observation** Attempted to gain access to a sensitive area with a temporary ID to determine whether access was denied.	No deviations noted. No deviations noted.
CC5.5.6	Keys to locked cabinets are restricted to authorized FORTRUST and customer personnel. A custody acknowledgement form must be signed by the recipient of the key and either the VP of Operations or the Facilities Manager.	**Inquiry and Observation** Inquired of management and observed locked cabinets to determine whether cabinets are restricted to authorized personnel. **Inspection** For a selection of new employees and customers granted keys to locked cabinets, inspected the corresponding FORTRUST Key Custody Acknowledgement Form to determine whether the form was signed by the employee/customer and approved by either the VP of Operations or the Facilities Manager.	No deviations noted. No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
Logical and Physical Access Controls Common Criteria 5.6 Description Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.6.1	Network access to routers and switches is provided from authorized FORTRUST IP addresses, using password authentication.	**Inquiry and Inspection** Inquired of management and inspected Active Directory password settings that control network access to routers and switches to determine whether passwords require a minimum length, are complex, and are required to change frequently. **Inspection** For a selection of routers, inspected the ACL settings to determine whether access is restricted to FORTRUST IP addresses, denying all others.	No deviations noted. No deviations noted.
CC5.6.2	Administrative access to the network routers and switches is restricted based on job responsibility.	**Inquiry and Inspection** Inquired of management and inspected user access listings within Active Directory, which controls access to all FORTRUST infrastructure, to determine whether administrative access is restricted based on job responsibility.	No deviations noted.
CC5.6.3	Any configuration changes made to routers are logged and automatically emailed to the Network Engineers and NOC Supervisor and saved on the syslog server.	**Inquiry and Inspection** Inquired of management and for a selection of routers, inspected system configurations to confirm that all routers are configured to notify the Network Engineers and NOC Supervisor of any changes. **Inspection** For a selection of routers, inspected a sample notification sent when a configuration change is made to the router to determine whether it was emailed as configured.	No deviations noted. No deviations noted.

5.0 Common Criteria Related to Logical and Physical Access Controls			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC5.6.4	Administrator access to the network and infrastructure monitoring tool, Nagios, is controlled through Active Directory. This access is restricted to the SVP/GM, VP of Operations, NOC Supervisor, System Administrator, Facilities and IT Managers, and Network Engineers.	**Inquiry and Inspection** Inquired of management and inspected the Domain Administrators in Active Directory to determine whether administrative access to Nagios is restricted to the SVP/GM, VP of Operations, NOC Supervisor, System Administrator, Facilities and IT Managers, and Network Engineers.	No deviations noted.
CC5.6.5	Access to the security system software controlling badge readers and biometric scanners to create and delete badges and change access parameters is limited to NOC personnel, the SVP/GM, VP of Operations, Facilities Manager, and Data Center Operations personnel.	**Inquiry and Inspection** Inquired of management and inspected the security system software user listing to determine whether access to create and delete badges and change access parameters is restricted to authorized personnel.	No deviations noted.
Logical and Physical Access Controls Common Criteria 5.7 Description The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security and availability.			
This criterion is not applicable to the services provided by FORTRUST.			
Logical and Physical Access Controls Common Criteria 5.8 Description Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.			
This criterion is not applicable to the services provided by FORTRUST.			

6.0 Common Criteria Related to System Operations			
System Operations Common Criteria 6.1 Description Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC6.1.1	The internal environment, servers, network equipment, and system capacity are monitored to detect and react to problems. Identified problems are tracked and monitored for resolution in a timely manner.	**Inquiry and Inspection** Inquired of management and observed the FORTRUST monitoring tools in place to determine whether the internal environment, servers, network equipment, and system capacity are monitored to detect and react to problems.	No deviations noted.
		Inspection Inspected a selection of tickets to determine whether identified problems are tracked and monitored for resolution in a timely manner.	No deviations noted.
System Operations Common Criteria 6.2 Description Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC6.2.1	Customer issues, internal issues, and Remote Hands requests are documented in the ticket system, escalated, and responded to in accordance with policy timelines. Customer requests must come from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of tickets and premises authorization forms to determine whether customer requested issues were authorized by approved customer personnel.	No deviations noted.

6.0 Common Criteria Related to System Operations			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC6.2.2	Procedures have been established and implemented to monitor customer support operations against defined customer service metrics. Management holds weekly staff meetings where open tickets are reviewed, issues are identified and discussed, and changes that may affect system security and availability are communicated to managers and users who could be affected.	**Inquiry** Inquired of management to determine whether procedures have been established and implemented to monitor customer support operations against defined customer service metrics.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether open tickets were reviewed and whether issues were identified and discussed.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security and availability are communicated to managers and users who could be affected.	No deviations noted.
CC6.2.3	Authorized customers, via the CORG, are instructed on submitting complaints and who to contact if they become aware of a possible security breach.	**Inquiry and Inspection** Corroborated with management and for a selection of customers, inspected the related CORG form for user entities to determine whether authorized customers were instructed on submitting complaints and who to contact if they become aware of a possible security breach.	No deviations noted.
CC6.2.4	Customer issues, internal issues, and Remote Hands requests are documented in the ticket system, escalated, and responded to in accordance with policy timelines. Customer requests must come from authorized customer personnel.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of tickets and premises authorization forms to determine whether customer requested issues were authorized by approved customer personnel.	No deviations noted.

7.0 Common Criteria Related to Change Management			
Change Management Common Criteria 7.1 Description Security and availability commitments and requirements are addressed during the system development lifecycle, including the design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC7.1.1	Changes to infrastructure servers or devices are authorized, documented, and tested and a back-out plan created. Customers are notified whether modifications impact their operations.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets for changes to infrastructure servers and devices to determine whether the changes were authorized, documented, tested, back-out plans were documented, and that customers affected by the changes were notified.	No deviations noted.
Change Management Common Criteria 7.2 Description Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security and availability.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC7.2.1	Any configuration changes made to routers are logged and automatically emailed to the Network Engineers and NOC Supervisor and saved on the syslog server.	**Inquiry and Inspection** Inquired of management and for a selection of routers, inspected system configurations to confirm that all routers are configured to notify the Network Engineers and NOC Supervisor of any changes. **Inspection** For a selection of routers, inspected a sample notification sent when a configuration change is made to the router to determine whether it was emailed as configured.	No deviations noted. No deviations noted.

7.0 Common Criteria Related to Change Management			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC7.2.2	FORTRUST maintains security policies that address both IT and physical security and availability policies that address the availability of the system. Policies and procedures are required to be periodically reviewed and approved by either the SVP of Operations or SVP/GM. The SVP of Operations is responsible for the system availability and related security policies.	**Inquiry and Inspection** Inquired of management and inspected FORTRUST's policies to determine whether security policies were in place that address both IT and physical security for the in-scope technology and whether availability policies were in place that address the availability of the system.	No deviations noted.
		Inquiry and Inspection Inquired of management to determine whether the SVP of Operations is responsible for the system availability and related security policies. For a selection of security and availability policies that were updated during the audit period, inspected documentation to determine whether the policies were reviewed and approved by either the SVP of Operations or SVP/GM.	No deviations noted.
		Inquiry and Inspection Inquired of management and inspected a selection of weekly management meeting minutes to determine whether changes that may affect system security are communicated to managers and users who could be affected.	No deviations noted.
CC7.2.3	Changes to infrastructure servers or devices are authorized, documented, and tested and a back-out plan created. Customers are notified whether modifications impact their operations.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets for changes to infrastructure servers and devices to determine whether the changes were authorized, documented, tested, back-out plans were documented, and that customers affected by the changes were notified.	No deviations noted.

7.0 Common Criteria Related to Change Management			
Change Management Common Criteria 7.3 Description Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC7.3.1	FORTRUST maintains a risk assessment and threat analysis for risks against the system. When high severity incidents or breaches are identified, a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. The risk assessment is updated annually or as needed based on significant events.	**Inquiry** Inquired of management to determine whether FORTRUST maintains a risk assessment and threat analysis for risks against the system. When high severity incidents or breaches are identified, a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. The risk assessment is updated annually or as needed based on significant events. **Inspection** For a selection of high severity tickets/breaches, inquired of management and inspected the risk assessment to determine whether a root cause analysis is performed and the risk assessment is updated to reflect the plan and resolution. **Inspection** Inspected the risk assessment to determine whether the assessment is updated on an annual basis or as needed based on significant events.	No deviations noted. No deviations noted. No deviations noted.
Change Management Common Criteria 7.4 Description Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and availability commitments and requirements.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC7.4.1	Any configuration changes made to routers are logged and automatically emailed to the Network Engineers and NOC Supervisor and saved on the syslog server.	**Inquiry and Inspection** Inquired of management and for a selection of routers, inspected system configurations to confirm that all routers are configured to notify the Network Engineers and NOC Supervisor of any changes. **Inspection** For a selection of routers, inspected a sample notification sent when a configuration change is made to the router to determine whether it was emailed as configured.	No deviations noted. No deviations noted.

7.0 Common Criteria Related to Change Management			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
CC7.4.2	Changes to infrastructure servers or devices are authorized, documented, and tested and a back-out plan created. Customers are notified whether modifications impact their operations.	**Inquiry and Inspection** Inquired of management and inspected a selection of tickets for changes to infrastructure servers and devices to determine whether the changes were authorized, documented, tested, back-out plans were documented, and that customers affected by the changes were notified.	No deviations noted.
CC7.4.3	Emergency maintenance requests require approval from the SVP/GM or VP of Operations in the SVP/GM's absence and are recommended by the Senior Network Engineer. When the maintenance is deemed to impact customers, those customers are notified as soon as possible and practical of the maintenance window prior to work being performed.	**Inquiry and Inspection** Inquired of management and inspected policies and procedures to determine whether procedures exist to provide that emergency changes are documented and authorized timely. **Inspection** For a selection of emergency changes, inspected documentation to determine whether changes were recommended by the Senior Network Engineer and approved by the SVP/GM or the Vice President of Operations, and whether customers were notified of the maintenance window timely, prior to work being performed.	No deviations noted. No deviations noted.

Additional Criteria for Availability			
Availability Additional Criteria 1.1 Description Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
A1.1.1	The NOC is staffed to provide customer support, monitoring, and Remote Hands support 24x7x365. The NOC uses network performance management monitoring tools to monitor all FORTRUST provided customer switch ports that connect to the Internet. Appropriate FORTRUST personnel are notified of identified problems, CRM tickets are opened, and problems are tracked to resolution.	**Observation** At multiple times during the audit period, observed the NOC utilize network performance management monitoring tools to monitor network performance.	No deviations noted.
		Inspection For a selection of days, inspected email notifications and walkthrough checklists to determine whether NOC personnel documented the performance of 24x7x365 monitoring as well as walkthroughs of the Data Center multiple times per day.	No deviations noted.
		Inspection Inspected email configuration settings within the syslog and network performance monitoring tools to determine whether FORTRUST personnel are automatically notified of identified problems. Inspected an example email to determine whether the email was sent based on the configuration.	No deviations noted.
		Observation Observed the configuration settings within the monitoring systems and the corresponding email to determine whether FORTRUST personnel are notified when the temperature and humidity levels go below an acceptable threshold.	No deviations noted.
		Inquiry and Observation Inquired of management and observed the monitoring system user listing to determine whether access is restricted to authorized FORTRUST personnel.	No deviations noted.
		Inspection Inspected a selection of tickets to determine whether the internal and customer requested issues were documented, escalated, and responded to in accordance with policy timelines.	No deviations noted.

Additional Criteria for Availability			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
A1.1.2	The Data Center maintains redundant links to the Internet.	**Inquiry and Inspection** Performed corroborative inquiry and inspected the network diagram for existence of redundant links to internet service providers. In addition, inspected contracts between FORTRUST and its four internet service providers to verify standing agreements between the parties.	No deviations noted.
Availability Additional Criteria 1.2 Description Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
A1.2.1	The Data Center is equipped with smoke detection and fire suppression equipment. Periodic checks and maintenance procedures are performed to test and validate the operation of the detection and suppression equipment.	**Observation and Inspection** Observed the smoke detection and fire suppression equipment and inspected a selection of maintenance logs for smoke detection and fire suppression equipment to determine whether periodic checks and maintenance procedures were documented as performed.	No deviations noted.
A1.2.2	A risk analysis is performed on an annual basis. Identified threats are assessed for validity, and appropriate actions are carried out based on the resulting assessment of risk. The process is documented and maintained, and remediation activities must be approved first by management.	**Corroborative Inquiry** Through corroborative inquiry with management, determined whether a risk analysis is performed periodically, identified threats are assessed for validity, and appropriate actions are carried out based on the resulting assessment of risk.	No deviations noted.
A1.2.3	The Data Center is equipped with a combination of UPS systems and generators in an N+1 configuration to provide continuous power in the event of a power outage. All back-up power systems are capable of maintaining continuous system services to the facility. Periodic checks and maintenance procedures are performed to test and validate the operation of the power management systems.	**Observation and Inspection** Observed the UPS systems and generators and inspected a selection of maintenance logs for UPS systems and generators to determine whether periodic checks and maintenance procedures were documented as performed.	No deviations noted.

Additional Criteria for Availability			
No.	Control Activity	Tests of Operating Effectiveness	Results of Testing
A1.2.4	Temperature and humidity are maintained throughout the Data Center through the use of air conditioning, humidity, water detection, and temperature sensors. Periodic checks and maintenance procedures are performed to confirm that HVAC equipment and humidity, temperature, and water detection sensors are working properly.	**Observation and Inspection** Observed that air conditioning, humidity, water detection, and temperature sensors are present throughout the Data Center and inspected a selection of maintenance logs for HVAC equipment, as well as humidity, water detection, and temperature sensors to determine whether periodic checks and maintenance procedures were documented as performed.	No deviations noted.
A1.2.5	The Data Center maintains redundant links to the Internet.	**Inquiry and Inspection** Performed corroborative inquiry and inspected the network diagram for existence of redundant links to internet service providers. In addition, inspected contracts between FORTRUST and its four internet service providers to verify standing agreements between the parties.	No deviations noted.
A1.2.6	Router and switch configuration back-ups are performed multiple times daily onto a file server.	**Inquiry and Inspection** Inquired of management and inspected the cron job back-up script to determine whether router and switch configurations are scheduled to be backed up to a file server daily. **Inspection** Due to the automated nature of the backup process, selected one day and determined whether back-ups of the router and switch configurations to the file server were performed according to the automated schedule and whether failed back-ups were rerun without errors.	No deviations noted. No deviations noted.
Availability Additional Criteria 1.3 Description Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.			
This criterion is not applicable to the services provided by FORTRUST.			

SECTION FIVE

OTHER INFORMATION PROVIDED BY FORTRUST
THAT IS NOT COVERED BY THE INDEPENDENT SERVICE AUDITOR'S REPORT

INTRODUCTION

The information included in Section Five of this report is presented by FORTRUST to provide additional information to user entities and is not part of FORTRUST's Description of its System. The information included here in Section Five has not been subjected to the procedures applied in the examination of the Description of the System; accordingly, EKS&H expresses no opinion on it.

No testing deviations were identified during this audit.

FORTRUST'S DISASTER RECOVERY PLAN

In order to ensure that, regardless of the situation, FORTRUST has established a formal Disaster Recovery Plan designed to provide uninterrupted service to all of its customers:

- FORTRUST's servers and systems are redundant on several layers.
- Nightly back-ups of all of FORTRUST's information systems are routinely created and stored securely offsite. In addition, FORTRUST continuously mirrors mission critical data to a secure, offsite data center.
- FORTRUST's facilities are equipped with uninterruptible power via onsite power generation and battery back-up that provide electricity to FORTRUST's entire building in the event of a power outage.
- Secure offsite back-up and records storage is provided by a third-party information storage provider.

FORTRUST's Disaster Recovery Plan also includes the following elements, as they relate to information technology:

- Plan activation and recovery team identification;
- Alternate offsite locations;
- Key contacts, vendors, and emergency numbers;
- Detailed system inventory;
- Critical business functions lists and priorities for resumption;
- Equipment, software and hardware lists, and priorities for recovery;
- Employee training and information packets; and
- Offsite procedures and recovery information.